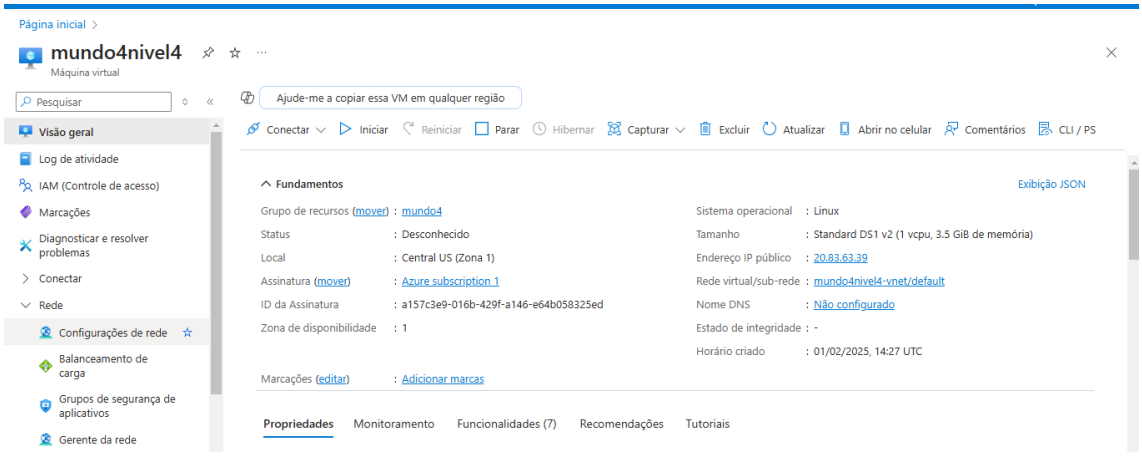
Microatividade 2: Configurar Regras de Rede e Grupos de Segurança no Azure

Material necessário:

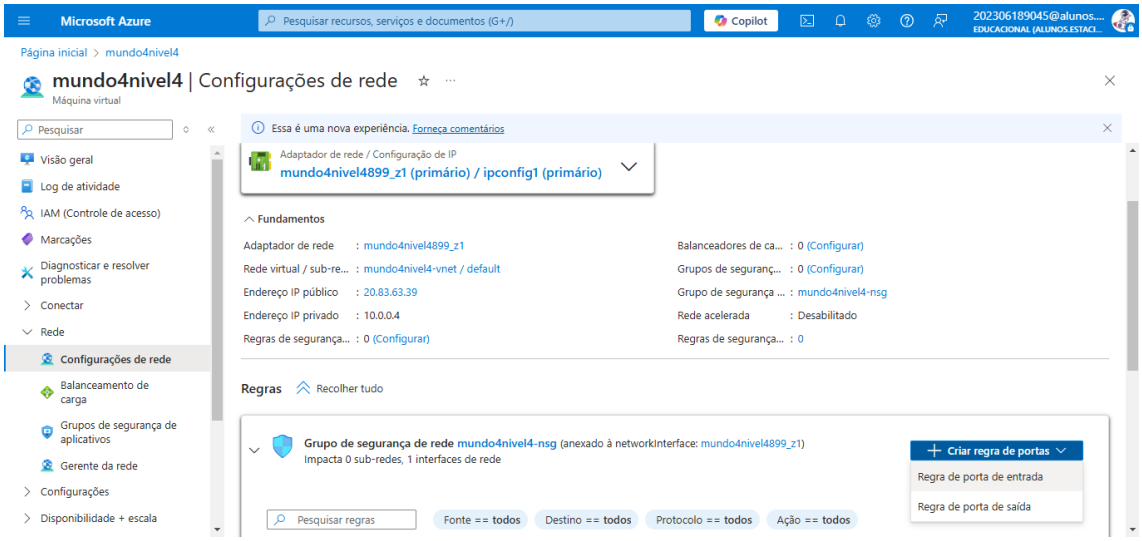
- Conta na Azure.
- Navegador Web: Google Chrome, Firefox, MS Edge, Safari ou Opera.

- Procedimentos

1. Acesse o portal do Azure utilizando seu navegador.
2. No painel de controle do Azure, clique na VM que você criou na Microatividade 1
3. para selecioná-la.
4. No menu lateral esquerdo, clique em "Configurações de Rede ".



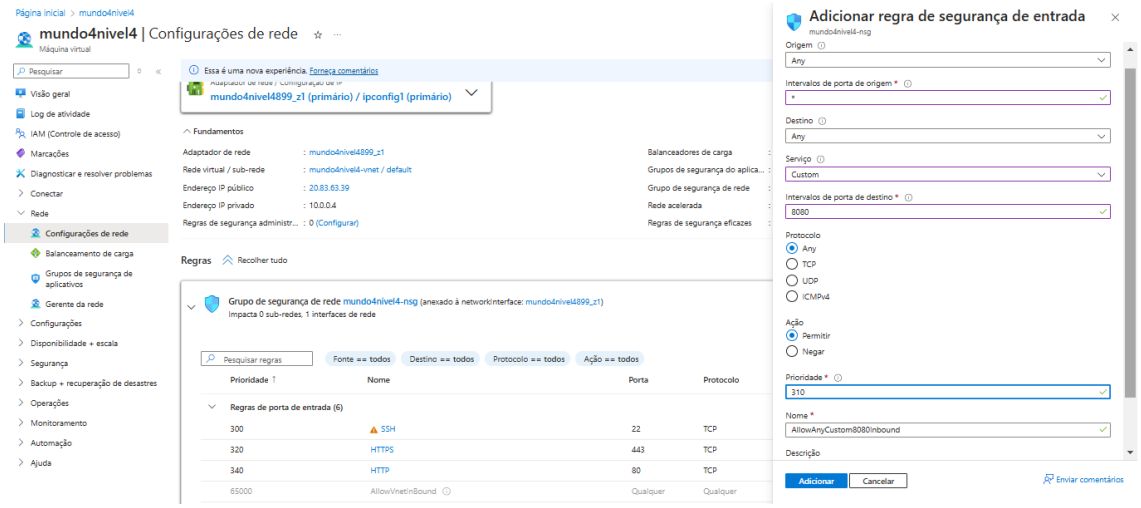
4. Na seção de "Grupo de segurança de rede", clique em "Criar regra de portas" para criar uma nova “Regra de portas de entrada”.



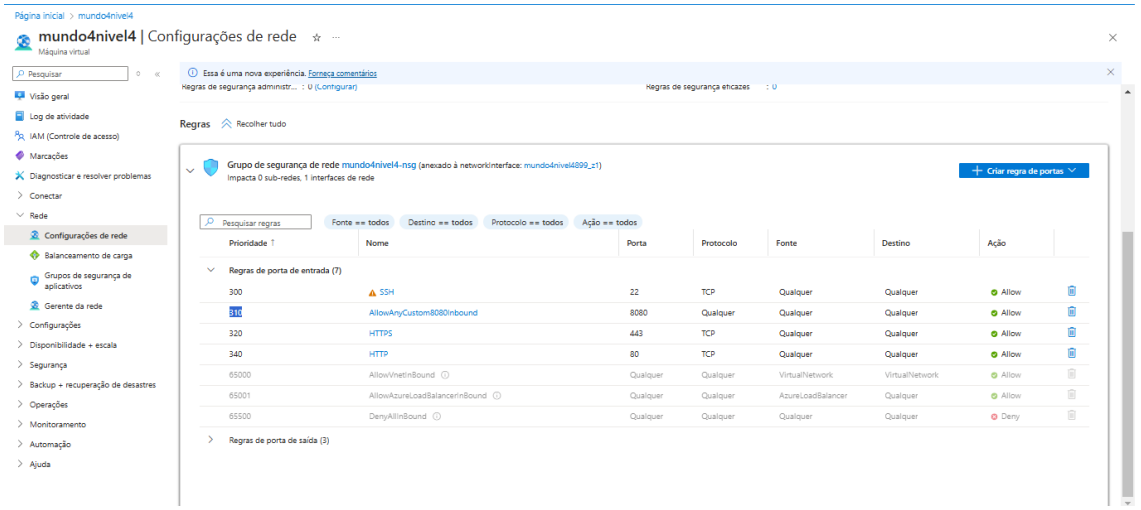
5. Crie uma regra para permitir que qualquer pessoa na internet possa acessar um servidor Web hospedado na máquina virtual criada anteriormente. Preencha os campos necessários para a regra, incluindo:

- Origem: O filtro de origem pode ser qualquer (any), um intervalo de endereços IP, meu endereço IP, um grupo de segurança de aplicativo ou uma marca padrão. Ele especifica o tráfego de entrada de um intervalo de endereços IP de origem específico que será permitido ou negado por essa regra.
- Intervalos de porta de origem: Forneça uma única porta, como, 80; um intervalo de portas, como, 1024 a 65535, ou uma lista separada por vírgulas de portas e/ou intervalos de portas únicos, como 80,1024-65535. Isso especifica de quais portas a entrada de tráfego será permitida ou negada por esta regra. Forneça um asterisco (*) para permitir o tráfego por meio de qualquer porta.

- Destino: O filtro de destino pode ser qualquer um, um intervalo de endereços IP, um grupo de segurança de aplicativos ou uma marca padrão. Ele especifica o tráfego de saída de um intervalo de endereços IP de destino específico que será permitido ou negado por essa regra.
- Serviço: O serviço especifica o protocolo de destino e o intervalo de porta para essa regra. Você pode escolher um serviço predefinido, como RDP ou SSH, ou fornecer um intervalo de porta personalizado. Se selecionar um serviço específico o próximo item (Intervalos de porta de destino) será preenchido com o valor padrão e não será editável.
- Intervalos de porta de destino: Somente editável se na opção anterior for marcado “Custom”. Forneça uma única porta, como, 80; um intervalo de portas, como, 1024 a 65535, ou uma lista separada por vírgulas de portas e/ou intervalos de portas únicos, como 80,1024-65535. Isso especifica de quais portas a entrada de tráfego será permitida ou negada por esta regra. Forneça um asterisco (*) para permitir o tráfego por meio de qualquer porta.
- Protocolo: Escolha entre as opções disponíveis (Any, TCP, UDP ou ICMP)
- Ação: selecione entre permitir ou negar
- Prioridade: ordem de processamento da regra. As regras são processadas em ordem de prioridade; quanto menor for o número, maior a prioridade. Recomendamos deixar lacunas entre as regras - 100, 200, 300, etc. - para que seja mais fácil adicionar novas regras sem ter que editar regras existentes.
- Nome da regra: Especifique um nome para a regra.
- Descrição: Preencha uma descrição da regra especificando a sua finalidade.



6. Após preencher todos os campos, clique em "Adicionar" para criar a regra. A figura a seguir exemplifica a regra criada.



- Resultados esperados

O resultado esperado desta microatividade é que o aluno seja capaz de configurar

com sucesso uma regra de segurança de rede no Azure para melhorar a segurança da

rede virtual utilizada pela VM criada na Microatividade 1. Certifique-se de que a regra

seja criada com as configurações desejadas.